UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/623,112 | 07/18/2003 | Gary G. Liu | 10664-166001 | 4468 |

26181          7590          04/30/2009
FISH & RICHARDSON P.C.
PO BOX 1022
MINNEAPOLIS, MN 55440-1022

| EXAMINER |
|---|
| LI, GUANG W |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2446 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 04/30/2009 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

| | Application No. | Applicant(s) |
|---|---|---|
| **Office Action Summary** | 10/623,112 | LIU, GARY G. |
| | Examiner | Art Unit | |
| | GUANG LI | 2446 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *30 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-4,7-11,14-23,28-51 and 56-58* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7-11,14-23,28-51 and 56-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08/20/2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date *11/18/2008*.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

## DETAILED ACTION

1.      It is hereby acknowledged that the following papers have been received and placed of record in the file: Amendment date 01/30/2009

2.      Claims 1-4, 7-11, 14-23, 28-51, 56-58 are presented for examination.

### *Response to Arguments*

3.      Applicant's arguments with respect to claims 1-4, 7-11, 14, 20-23, 33-51 have been considered but are moot in view of the new ground(s) of rejection.

4.      Applicant's arguments filed 01/30/2009 regarding claim 15-19, 28-32 and 56-58 have been fully considered but they are not persuasive.

5.      Applicant argues the following limitation(s):

   •      Applicant argues, stated in the remark on page 13, "Fleming's personal authorized sender list is retained by a local employee, and is not distributed to anyone in the email network because the sender list is "personalized". Because Fleming does not distribute the personal authorized sender list to any other individual, a sender's status (e.g., whether the sender is an authorized sender) is only known to the individual employee who authorizes the sender to send messages. See col. 5, lines 17-19". On the contrary, Fleming discloses the administrator could maintain a global authorized sender list that is shared by all employees. Each employee could also maintain a personal authorized sender list the identifies additional senders (e.g., spouse) who are authorized to send electronic mail messages to the employee. The global authorized sender list includes the list of the authorized sender status whether the sender is authorized or not. If the

sender is authorized, the authorization component notifies the all the employee personal

authorized list whether that particular sender status (see Fleming: col.5 lines 1-20).

- Applicant argues, stated in the remark on page 16, "There is no indication that

Goodman collects any information from a plurality of spam filters. Rather, Goodman extracts

information from an outbound email, where the outbound email is sent to an intended recipient

only after the administrator has determined that the outbound email is not a spam email based on

the overall score assigned to the outbound email." On the contrary, Goldman teaches if the sum

total per outgoing message exceeds some threshold amount, then that message and/or the

respective sender can be flagged as a potential spammer (see Goldman: ¶[0011]). Goldman

providing the system and methods for effectively managing electronic messages and reducing the

number of unwanted messages. Therefore, it does provide using the collecting information to

reducing the unwanted messages. In another word, Goodman collecting information from

message filters to determine whether flagged a potential spammer or not. The information

collecting regarding filtering the emails that associated with sender are collected to determine

whether is a spammer or not.

- Applicant argues, stated in the remark on page 17, "Rounthwaite does not identify

a spammer based on these criteria. Rather, Rounthwaite identifies a spammer based on votes and

feedbacks collected from the recipients (8:3-10). User votes and feedbacks, however, are not

information collected from a plurality of spam filters, but each individual user". On the contrary,

Pickup teaches identifying and intercepting an unauthorised electronic mail before delivery to the

recipient, the unauthorised electronic mail being identified through a comparison of details of the

sender with details contained on a list of authorised senders (see Pickup: ¶[0009]) and

Rounthwaite teaches there may be limitations on the number of messages selected per user or per

user per time period, or on the probability of selecting a message from any given user to teach

the determining a trend in the collected information. In addition, Applicant admits the

Rounthwaite identified a spammer based on votes and feedbacks collected from the recipients

that stated a trend in the collection information can be vote and feedbacks that clearly teach

determined a trend in the collection information. Since Pickup teaches the identifying and

intercepting an unauthorized electronic mail before delivery to the recipient and Rounthwaite

teaches determining a trend in the collect information. It would have been obvious to one of

ordinary skill in the art, having the teachings of Pickup Through before them at the time the

invention was made to modify the method and system for detecting spam of Pickup to include

collection trend of information for spam prevention (Rounthwaite: col.1 lines 64 - col.2 lines 5).

In addition, Applicant does not clearly define how the trend determines in the collected

information based on. Applicant <u>only</u> claims the determining a trend <u>in</u> the collected information

not based on the collected information. In response to applicant's argument that the references

fail to show certain features of applicant's invention, it is noted that the features upon which

applicant relies (i.e., how the trend determines in the collected information based on) are not

recited in the rejected claim(s). Although the claims are interpreted in light of the specification,

limitations from the specification are not read into the claims. See *In re Van Geuns*, 988

F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

### *Claim Rejections - 35 USC § 103*

6.      The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

7.      Claims 1-4, 8-11, 14 and 33-44 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Pickup (US 2003/0212791 A1) in view of Fleming (US 6,249,805) in view of Abkemeier

(US 2003/0023736 A1).

8.      Regarding claim 1, Pickup teaches a method for detecting spam in a messaging system

comprising:

generating a white list of confirmed message senders (updating a whitelist containing

details of a recipient's authorised senders see ¶[0026]), each of said confirmed message senders

being authorized to send messages as evidenced by prior receipt of a response to a confirmation

message ("the sender is added to the list of authorised senders and the electronic mail is

forwarded to the recipient" see¶[0011]);

using the white list at a given one of the plurality of spam filters to determine if a sender

of a received message has been previously confirmed ("the request for verification sent to the

recipient can be forwarded only if received within a predetermined time of the recipient sending

a message to the sender. This will allow the recipient to "match" requests for verification with

emails that they have previously sent" see ¶[0021]); and

forwarding the received message to a recipient without separately confirming the sender

if it is determined that the sender has been previously confirmed ("Where verification is

received, the sender is added to the recipient's whitelist and further emails from the sender can be

delivered to the recipient without the requirement for a verification step" see ¶0063]).

Pickup does not explicitly disclose distributing the white list among a plurality of spam

filters in the messaging system.

However Fleming teaches the distributing the white list among a plurality of spam filters in the messaging system (global authorized sender list that are share among with employee authorized lists "the administrator could maintain a global authorized sender list that is shared by all employee" see Fleming: Col.5 line 1-10) in order to provide de-spamming services to the email system (Fleming: col.3 line 20-23).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Pickup to include (or to use, etc.) distributing the white list among a plurality of spam filters in the messaging system as taught by Fleming in order to in order to provide de-spamming services to the email system (Fleming: col.3 line 20-23).

Pickup together with Fleming does not explicitly disclose without separately confirming the sender by any other spam filter in the messaging system.

However Abkemeier teaches the without separately confirming the sender by any other spam filter in the messaging system (General share sender-based whitelist filter that general share sender-based white filter sharing the filtering data with individual user filters and pre-authorization to a given list of senders based on message criteria see Abkemeier: ¶[0039]; ¶[0048];¶[0050]). Abkemeier further teaches distributing the white list among a plurality of spam filter in the messaging system (Whitelist filtering is also available commonly available email service such as outlook and hotmail as a junk mail filter option which global whitelist supplies to the individual user for message filtering see Abkemeier: ¶[0008]; ¶[0048]) in order to easily mange and maintained (see Abkemeier: ¶[0018]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Pickup to include (or to use, etc.) the without separately confirming the

sender by any other spam filter in the messaging system as taught by Fleming in order to in order

to easily mange and maintained (see Abkemeier: ¶[0018]).

9.      Regarding claim 2, Pickup through Abkemeier taught the method for detecting spam

according to claim 1, as described above. Pickup further teaches wherein the messaging system

is an email system (system for authorizing electronic mail see Pickup: ¶[0001]).

10.     Regarding claim 3, Pickup through Abkemeier taught the method for detecting spam

according to claim 1, as described above. Fleming further teaches wherein distributing the white

list includes distributing the white list with at least two spam filters (global authorized sender list

that are share among with employee authorized lists "the administrator could maintain a global

authorized sender list that is shared by all employee" see Fleming: Col.5 line 1-10).

11.     Regarding claim 4, Pickup through Abkemeier taught the method for detecting spam

according to claim 1, as described above. Pickup further teaches wherein if the sender has not

been previously confirmed (a system for authorising electronic mail sent by an unauthorised

sender to a recipient see Pickup: ¶[0035]), the method further includes:

        sending a confirmation to the sender (send a request for verification to the sender of an

unauthorised email see Pickup: ¶[0039]);

        verifying a response from the sender (wherein upon receipt of the verification from the

sender see Pickup: ¶[0040]); and

        if the response is verified, adding the sender to the white list at the given spam filter (the

whitelist is modified to include the sender's details and the electronic mail is forwarded to the

recipient see Pickup: ¶[0040]) and sharing the information associated with the added sender with

other spam filters in the messaging system (In an alternative form to this, a plurality of recipients

share the same list of authorised senders" see Pickup: ¶0016]).

12.      Regarding claim 8, Pickup teaches a method for identifying a spam message comprising:

         receiving a message at a spam filter in a network that includes a plurality of spam filters,

each spam filter having an associated list of confirmed senders (share the same list of authorized

senders in each recipient "there are a plurality of recipients, and each recipient has a list of

authorised senders. In an alternative form to this, a plurality of recipients share the same list of

authorised senders" see Pickup: ¶[0016]);

         identifying the sender of the message (check the message after receiving message see

Fig.1);

         determining if the sender has been previously confirmed as a confirmed sender including:

         determining, if the sender is includes a list of confirmed senders associated with any

other spam filter in the network (After checking the recipient white list senders then go back to

check the System-wide white sender list where all the recipients share authorizes list of users see

Fig.1; ¶[0061]); and

         if so, forwarding the received message to a recipient without separately confirming the

sender in each spam filter (If the sender in the system-wide whitelist sender or recipient whitelist

sender, the message will deliver email to recipient see Pickup: Fig.1; ¶[0061] ).

         Pickup does not explicitly disclose using a locally stored list of confirmed senders.

         However Fleming teaches using a locally stored list of confirmed senders (personal

authorized sender list that confirmed by individual employee "Each employee could also

maintain a personal authorized sender list the identifies additional senders (e.g., spouse) who are

authorized to send electronic mail messages to the employee" see Fleming: col.5 lines 10-14) in order to provide de-spamming services to the email system (Fleming: col.3 line 20-23).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Pickup to include (or to use, etc.) using a locally stored list of confirmed senders as taught by Fleming in order to in order to provide de-spamming services to the email system (Fleming: col.3 line 20-23).

Pickup together with Fleming does not explicitly disclose if it is determined that the sender is included in the list of confirmed senders associated with any other spam filter in the network.

However Abkemeier teaches if it is determined that the sender is included in the list of confirmed senders associated with any other spam filter in the network (General share sender-based whitelist filter that general share sender-based white filter sharing the filtering data with individual user filters  and the authorized sender in the whitelist see Abkemeier: ¶[0039]; ¶[0048];¶[0050]). Abkemeier further teaches determining using a locally stored list of confirmed senders (pre-authorization to a given list of sender and separate filter for each user see Abkemeier: ¶[0008]; ¶[0048]) in order to easily mange and maintained (see Abkemeier: ¶[0018]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Pickup to include (or to use, etc.) if it is determined that the sender is included in the list of confirmed senders associated with any other spam filter in the network as taught by Fleming in order to in order to easily mange and maintained (see Abkemeier: ¶[0018]).

13.     Regarding claim 9, Pickup through Abkemeier taught the method for detecting spam according to claim 8, as described above. Pickup further teaches the messaging system is an email system (system for authorizing electronic mail see Pickup: ¶[0001]).

14.     Regarding claim 10, Pickup through Abkemeier taught the method for detecting spam according to claim 8, as described above. Pickup further comprising sharing the locally stored list of confirmed senders associated with another spam filter (the recipient whitelist senders and with system wide-white list sender shared the same authorized senders "In an alternative form to this, a plurality of recipients share the same list of authorised senders" see Pickup: Fig.1; ¶[0061]).

15.     Regarding claim 11, Pickup through Abkemeier taught the method for detecting spam according to claim 8, as described above. Pickup further teaches if is determined that the sender has not been previously confirmed (a system for authorising electronic mail sent by an unauthorised sender to a recipient see Pickup: ¶[0035]), the method further comprising:

        sending a confirmation to the sender (send a request for verification to the sender of an unauthorised email see Pickup: ¶[0039]);

        verifying a response from the sender (wherein upon receipt of the verification from the sender see Pickup: ¶[0040]); and

        if the response is acceptable, adding the sender to the locally stored list of confirmed senders (adding sender to recipient whitelist  see Fig.1 and Fig.2 "the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient" see Pickup: ¶[0040]) and sharing information with at least one other spam filter (shared authorized users with the system wide whitelist in the network see Pickup: Fig.1; ¶[0061])  in the network, the

information including information indicating that the sender has been confirmed (In an

alternative form to this, a plurality of recipients share the same list of authorised senders" see

Pickup: ¶0016]).

16.      Regarding claim 14, Pickup through Abkemeier taught the method for detecting spam

according to claim 8, as described above. Fleming and Pickup further teach wherein if the sender

has not been previously confirmed, the method further comprising:

    sending a confirmation to the sender (send a request for verification to the sender of an

unauthorised email see Pickup: ¶[0039]);

    verifying a response (wherein upon receipt of the verification from the sender see Pickup:

¶[0040]); and

    if the response is acceptable, adding the sender to the locally stored list; and distributing

the locally stored list among the plurality of spam filters (global authorized sender list that are

share among with employee authorized lists and authorized personal lists share global authorized

sender list to allow individual authorized sender in the personal list "the administrator could

maintain a global authorized sender list that is shared by all employees. Each employee could

also maintain a personal authorized sender list the identifies additional senders (e.g., spouse) who

are authorized to send electronic mail messages to the employee" see Fleming: Col.5 line 1-14).

17.      Regarding claim 33, Pickup teaches a method for filtering spam in a messaging system

(method of authorizing electronic mail sent by a sender to recipient see abstract) comprising:

    confirming that a message sender can receive one or more messages (Send verification

request back to sender block see fig.1);

using said information at a given one of the plurality of spam filters to determine if a message should be sent to an intended recipient without separately determining whether the message sender can receive one or more messages (wherein upon receipt of the verification from the sender, the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[0040]).

Pickup does not explicitly disclose distributing information indicating that the message sender can receive one or more messages among a plurality of spam filters in the messaging system.

However Fleming teaches the distributing information indicating that the message sender can receive one or more messages among a plurality of spam filters in the messaging system (message can either received authorization from global authorized sender list or personal authorized sender list "the administrator could maintain a global authorized sender list that is shared by all employee" see Fleming: Col.5 line 1-10) in order to provide authorization services to the email system (Fleming: col.3 line 20-23).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Pickup to include (or to use, etc.) distributing the white list among a plurality of spam filters in the messaging system as taught by Fleming in order to in order to provide authorization services to the email system (Fleming: col.3 line 20-23).

Pickup together with Fleming does not explicitly disclose determining by a local receiving spam filter and among a plurality of spam filters.

However Abkemeier teaches determining by a local receiving spam filter and among a plurality of spam filters and among a plurality of spam filters (General share sender-based

<u>whitelist filter</u> that general share sender-based white filter sharing the filtering data with

<u>individual user filters</u> and pre-authorization to a given list of senders based on message criteria

see Abkemeier: ¶[0039]; ¶[0048];¶[0050]). Abkemeier further teaches distributing the white list

among a plurality of spam filter in the messaging system (Whitelist filtering is also available

commonly available email service such as outlook and hotmail as a junk mail filter option which

global whitelist supplies to the individual user for message filtering see Abkemeier: ¶[0008];

¶[0048]) in order to easily mange and maintained (see Abkemeier: ¶[0018]).

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Pickup to include (or to use, etc.) by a local receiving spam filter and

among a plurality of spam filters and among a plurality of spam filters as taught by Fleming in

order to in order to easily mange and maintained (see Abkemeier: ¶[0018]).

18.     Regarding claim 34, claim 34 is rejected for the same reason in claim 2 as set forth

hereinabove.

19.     Regarding claim 35, Pickup through Abkemeier taught the method for detecting spam

according to claim 33, as described above. Pickup further comprising confirming at a first spam

filter in the system that a sender of a message can receive messages ("verification means

operating, upon detection of an unauthorized email, to send a request for verification to the

sender of an authorized email" see Pickup: ¶[0039]).

20.     Regarding claim 36, Pickup through Abkemeier taught the method for detecting spam

according to claim 35, as described above. Pickup further comprising receiving the message at a

second spam filter (Electronic message received at the first system-wide filters (Whitelist and

blacklist) and process to recipient filters (whitelist and blacklist see Pickup: Fig.1; ¶[0061]).

21.     Regarding claim 37, Pickup through Abkemeier taught the method for detecting spam according to claim 33, as described above. Fleming further teaches distributing information developed by the first spam filter with one or more other spam filters in the messaging system (create the global authorized sender list and share with all employee "the administrator could maintain a global authorized sender list that is shared by all employees. Each employee could also maintain a personal authorized sender list the identifies additional senders (e.g., spouse) who are authorized to send electronic mail messages to the employee" see Fleming: Col.5 line 1-14).

22.     Regarding claim 38, Pickup through Abkemeier taught the method for detecting spam according to claim 37, as described above. Pickup further comprising distributing the information with a data center (the mail server is located outside of a network associated with the recipient see Pickup: ¶[0047]) and thereafter allowing access by each of the spam filters in the messaging system to the information (share the system-wide whitelist with all other recipients in the network see Pickup: ¶[0016]).

23.     Regarding claim 39, Pickup through Abkemeier taught the method for detecting spam according to claim 33, as described above. Pickup further teaches wherein the information is maintained in a list that includes one or more confirmed message senders ("there are a plurality of recipients, and each recipient has a list of authorised senders" see Pickup: ¶[0016]).

24.     Regarding claim 40, Pickup through Abkemeier taught the method for detecting spam according to claim 39, as described above. Fleming further teaches wherein the list is distributed among with a plurality of the spam filters in the messaging system (the global authorized sender list and share with all employee "the administrator could maintain a global authorized sender list that is shared by all employees. Each employee could also maintain a personal authorized sender

list the identifies additional senders (e.g., spouse) who are authorized to send electronic mail

messages to the employee" see Fleming: Col.5 line 1-14).

25.     Regarding claim 41, Pickup through Abkemeier taught the method for detecting spam

according to claim 39, as described above. Pickup further teaches wherein the list  (System-wide

whitelist see Pickup: Fig.1) is maintained by a data center (the mail server is located outside of a

network associated with the recipient see Pickup: ¶[0047]) accessible by the spam filters in the

messaging system (share the system-wide whitelist with all other recipients in the network see

Pickup: ¶[0016]).

26.     Regarding claim 42, Pickup through Abkemeier taught the method for detecting spam

according to claim 41, as described above. Fleming further teaches distributing the list with a

plurality of spam filters in the messaging system (the global authorized sender list and share with

all employee "the administrator could maintain a global authorized sender list that is shared by

all employees. Each employee could also maintain a personal authorized sender list the identifies

additional senders (e.g., spouse) who are authorized to send electronic mail messages to the

employee" see Fleming: Col.5 line 1-14).

27.     Regarding claim 43, Pickup through Abkemeier taught the method for detecting spam

according to claim 37, as described above. Pickup further teaches maintaining a copy of the list

at one or more of the of spam filters in the messaging system (list been keep update in the

system-wide whitelist "continuously updating a list of authorized senders to filter unwanted

electronic mail" see Pickup:  ¶[0027]).

28.     Regarding claim 44, Pickup through Abkemeier taught the method for detecting spam

according to claim 37, as described above. Pickup further teaches associating a passcode with

one or more of the confirmed senders in the list, and verifying a message received from a sender

in the list including verifying the passcode specified by the sender (a non-machine readable code

for sender verification "utilise a request for verification where that request includes non-machine

readable code to make it difficult for automated verification of the message" see Pickup:

¶[0022]).

29.    **Claims 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pickup (US**

**2003/0212791 A1) in view of Fleming (US 6,249,805) in view of Abkemeier (US**

**2003/0023736 A1) in further view of McCormick et al. (US 6,023,723).**

30.    Regarding claim 7, Pickup through Abkemeier taught the method for detecting spam

according to claim 1, as described above. Pickup further teach wherein the if the sender has not

been previously confirmed, the method further comprising:  sending a confirmation to

sender(send a request for verification to the sender of an unauthorised email see Pickup:

¶[0039]); verifying a response from the sender (wherein upon receipt of the verification from the

sender see Pickup: ¶[0040]); and if the response is verified, adding the sender to the white list

maintained at a central location that is distributed among the plurality of spam filters (the

whitelist is modified to include the sender's details and the electronic mail is forwarded to the

recipient see Pickup: ¶[0040]).

         Pickup through Abkemeier does not explicitly disclose white list maintained a central

location.

         However McCormick teaches white list maintained a central location (address filter

server 22 at the remote central location 46 see McCormick col. 4 lines 49-51) in order to

effectively filtered by the user as will compiling a update master list of unwanted e-email

transmitters (McCormick: Col.2 lines 36-40).

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Pickup through Abkemeier to include (or to use, etc.) white list

maintained a central location as taught by Fleming in order to in order to effectively filtered by

the user as will compiling a update master list of unwanted e-email transmitters (McCormick:

Col.2 lines 36-40).

31.     **Claims 20-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pickup**

**(US 2003/0212791 A1) in view of McCormick et al. (US 6,023,723) further in view of**

**Abkemeier (US 2003/0023736 A1).**

32.     Regarding claim 20, Pickup teaches a method for detecting spam in a messaging system

comprising:

generating a list of confirmed message senders (updating a whitelist containing details of

a recipient's authorised senders see Pickup: ¶[0026]) and maintaining the list (To automatically

update the whitelist, the recipient can utilise the automatic updating mechanism see Pickup:

¶[0062]) at a data center (the mail server is located outside of a network associated with the

recipient see Pickup: ¶[0047]);

receiving a message at a spam filter in a network that includes a plurality of spam

filters(share the same list of authorized senders in each recipient "there are a plurality of

recipients, and each recipient has a list of authorised senders. In an alternative form to this, a

plurality of recipients share the same list of authorised senders" see Pickup: ¶[0016]);

the sender of the message is a confirmed message sender (system-wide whitelist sender

and global whitelist see Pickup: ¶[0064]), and

if it is determined that the sender is a confirmed message sender, forwarding the received

message to a recipient without separately confirming the sender (the whitelist is modified to

include the sender's details and the electronic mail is forwarded to the recipient see Pickup:

¶[0040]).

Pickup does not explicitly disclose verifying with the data center by the spam filter.

However McCormick teaches the verifying with the data center by the spam filter.

(verifying address filter server 22 at the remote central location 46 by the automatic discard filter

see McCormick col. 4 lines 49-51) in order to effectively filtered by the user as will compiling a

update master list of unwanted e-email transmitters (McCormick: Col.2 lines 36-40).

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Pickup to include (or to use, etc.) verifying with the data center by the

spam filter as taught by Fleming in order to in order to effectively filtered by the user as will

compiling a update master list of unwanted e-email transmitters (McCormick: Col.2 lines 36-40).

Pickup together with McCormick does not explicitly disclose confirmed message sender

of one of the plurality of spam filters other than the spam filter.

However Abkemeier teaches confirmed message sender of one of the plurality of spam

filters other than the spam filter. (General share sender-based whitelist filter that general share

sender-based white filter sharing the filtering data with individual user filters and pre-

authorization to a given list of senders based on message criteria see Abkemeier: ¶[0039];

¶[0048];¶[0050]). Abkemeier further teaches distributing the white list among a plurality of spam

filter in the messaging system (Whitelist filtering is also available commonly available email service such as outlook and hotmail as a junk mail filter option which global whitelist supplies to the individual user for message filtering see Abkemeier: ¶[0008]; ¶[0048]) in order to easily mange and maintained (see Abkemeier: ¶[0018]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Pickup to include (or to use, etc.) the confirmed message sender of one of the plurality of spam filters other than the spam filter as taught by Fleming in order to in order to easily mange and maintained (see Abkemeier: ¶[0018]).

33.     Regarding claim 21, Pickup together with Abkemeier taught the method for detecting spam according to claim 20, as described above. Pickup further teaches the messaging system is an email system (system for authorizing electronic mail see Pickup: ¶[0001]).

34.     Regarding claim 22, Pickup together with Abkemeier teaches the method of claim 20 as described hereinabove. Pickup further comprising sharing the list with at least two spam filters in the network (two or more recipients share the same list "there are a plurality of recipients, and each recipient has a list of authorised senders. In an alternative form to this, a plurality of recipients share the same list of authorised senders" see Pickup: ¶0016]).

35.     Regarding claim 23, Pickup together with Abkemeier teaches the method of claim 20 as described hereinabove. Pickup further teach if it is determined that the sender is not a confirmed message sender, the method further comprising:

sending, from the data center, a confirmation to the sender (forwarding a request for verification to the sender see Pickup: ¶[0025]); verifying a response received at the data center

from the sender (verification means operating, upon detection of an  unauthorized email, to send

a request for verification to the sender of an authorized email see Pickup: ¶[0039])

if the response is acceptable, adding to the list of confirmed message senders  a name

associated with the sender(wherein upon receipt of the verification from the sender, the whitelist

is modified to include the sender's details and the electronic mail is forwarded to the recipient see

Pickup: ¶[0040]); and sharing information including the name with other spam filters in the

network (a plurality of recipients share the same list of authorised senders see Pickup: ¶0016]).

36.      **Claims 15-19 and 28-32 are rejected under 35 U.S.C. 103(a) as being unpatentable**

**over Pickup (US 2003/0212791 A1) in view of Rounthwaite et al. (US 7,219,148) and further**

**in view of Goldman et al. (US 2005/0021649 A1)**

37.      Regarding claim 15, Pickup teaches a method for detecting a spammer in a network that

includes a plurality of spam filters, the method comprising: collecting information relating from

a plurality of the spam filter (identifying and intercepting an unauthorised electronic mail before

delivery to the recipient, the unauthorised electronic mail being identified through a comparison

of details of the sender with details contained on a list of authorised senders see Pickup:

¶[0009]).

Rounthwaite teaches determining a trend in the collected information; and identifying a

spammer based on the trend (determining spammer based on the limitations "there may be

limitations on the number of messages selected per user or per user per time period, or on the

probability of selecting a message from any given user. Without such limits, a spammer could

create an account" see Rounthwaite: col.6 lines 62-66).

Rounthwaite further provides the advantage of Users which are identified as spam-fighter are asked to vote on whether a selection of their incoming email messages is individually either legitimate mail or junk mail (see Abstract).

Pickup together with Rounthwaite does not explicitly disclose collecting information relating to a sender.

Goldman teaches the collecting information relating to a sender (collecting outgoing message of the sender to determined whether is a spammer or not "If the sum total per outgoing message exceeds some threshold amount, then that message and/or the respective sender can be flagged as a potential spammer" see Goldman: ¶[0011]).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup Through before them at the time the invention was made to modify the method and system for detecting spam of Pickup to include collecting information relating to a sender as taught by Goldman.

One of ordinary skill in the art would have been motivated to make this modification in order to improve spam-detecting system based on sender actions in view of Goldman.

38.     Regarding claim 16, Pickup through Goldman taught the method for detecting spam according to claim 15, as described above. Rounthwaite further teaches collecting information includes collecting information relating to a number of messages sent by a sender to unrelated email addresses (there may be limitations on the number of messages selected per user" see Rounthwaite: col.6 lines 62-63).

39.     Regarding claim 17, Pickup through Goldman taught the method for detecting spam according to claim 15, as described above. Rounthwaite further teaches determining trends

includes correlating the messages received by an individual spam filter relating to a same sender

(to detect as spammer based on the probability of selecting a message from any given user see

Rounthwaite: col.6 lines 62-65).

40.     Regarding claim 18, Pickup through Goldman taught the method for detecting spam

according to claim 15, as described above. Rounthwaite further teaches identifying includes

determining that a sender is a spammer if a number of messages sent to unrelated email

addresses exceeds a predetermined threshold (the disagreement vote all based on individual user

action to vote whether the message is legitimate or spam "the number disagreements exceeds a

threshold level, then the suspect users is consider untrustworthy" see Rounthwaite: col. 19 lines

54-56).

41.     Regarding claim 19, Pickup through Goldman taught the method for detecting spam

according to claim 15, as described above. Rounthwaite further teaches the threshold is time

dependent (time period can be set in advance or the message can be held until receipt of a

determined number of poll results similar to the message e.g. from the same IP address or with

similar content see Rounthwaite: col.3 line 67 – col.4 lines 1-3).

42.     Regarding claim 28, claim 28 is rejected for the same reason as claim 15 as set forth

hereinabove. Pickup further teaches collecting information using data center (System-wide

whitelist or Global whitelist that hosting in the network for identifying the sender permission see

Pickup: ¶ [0064]).

43.     Regarding claim 29, claim 29 is rejected for the same reason as claim 16 as set forth

hereinabove.

44.    Regarding claim 30, claim 30 is rejected for the same reason as claim 17 as set forth

hereinabove.

45.    Regarding claim 31, claim 31 is rejected for the same reason as claim 18 as set forth

hereinabove.

46.    Regarding claim 32, claim 32 is rejected for the same reason as claim 19 as set forth

hereinabove.

47.    Claims 56-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pickup (US

2003/0212791 A1) in view of Fleming (US 6,249,805).

48.    Regarding claim 56, Pickup teaches a method for minimizing spam in a messaging

system, the messaging system including a plurality of spam filters, the method comprising:

        to verify if a sender of a message is a confirmed sender, a confirmed sender being a

sender having a verified capability to receive messages; evaluating a list of confirmed senders

(confirmation and verification of confirmed user "identifying an unauthorised electronic mail,

the unauthorised electronic mail being addressed to the recipient and originating from a sender

whose details are not included on the whitelist, forwarding a request for verification to the

sender, receiving verification from the sender and including the sender's details on the whitelist"

see Pickup:¶[0028-0030]);

        if the sender is not included in the list of confirmed senders , confirming the sender

including providing a notification to the sender (Send verification request back to the sender see

Fig.1; ¶[0061] and

upon receipt of a confirmation from the sender in response to the notification, including

adding the sender to the list (forwarding a request for verification to the sender and receiving

verification from the sender and including the sender's details on the whitelist see Pickup:

¶[0025-0026]); and

notifying the one spam filter indicating whether the sender's status is confirmed (the

plurality of recipients share the same list notify each other whether the sender is authorized user

or not "there are a plurality of recipients, and each recipient has a list of authorised senders. In an

alternative form to this, a plurality of recipients share the same list of authorised senders" see

Pickup: ¶0016]).

Pickup does not explicitly disclose receiving a request from one of the spam filters in the

messaging system and distributing the sender's status with other spam filters in the messaging

system.

However Fleming teaches the receiving a request from one of the spam filters in the

messaging system and distributing the sender's status with other spam filters in the messaging

system (send the personal authorization list to confirm the sender is authorized with personal list

"the administrator could maintain a global authorized sender list that is shared by all employees.

Each employee could also maintain a personal authorized sender list the identifies additional

senders (e.g., spouse) who are authorized to send electronic mail messages to the employee" see

Fleming: col.5 lines 10-14)" see Fleming: Col.5 line 1-10) in order to provide de-spamming

services to the email system (Fleming: col.3 line 20-23).

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Pickup to include (or to use, etc.) receiving a request from one of the

spam filters in the messaging system and distributing the sender's status with other spam filters in

the messaging system as taught by Fleming in order to in order to provide de-spamming services

to the email system (Fleming: col.3 line 20-23).

49.      Regarding claim 57, Pickup together with Fleming taught the method for detecting spam

according to claim 56, as described above. Pickup further teaches wherein the step of confirming

the sender is performed by a spam filter (Each recipient have individual whitelist and black list

"each recipient has a list of authorised senders" see Pickup: ¶[0016]; Fig.1).

50.      Regarding claim 58, Pickup together with Fleming taught the method for detecting spam

according to claim 56, as described above. Pickup further teaches wherein the step of confirming

the sender is performed by the requesting spam filter (sender went though the inbound e-mail

flowchart for filtering service and send verification message back to sender for confirmation see

Pickup: Fig.1).

51.      **Claims 45-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pickup**

**(US 2003/0212791 A1) in view of Fleming et al. (US 6,249,805) in view of Abkemeier (US**

**2003/0023736 A1) and further in view of Brown et al. (US 2004/0034694 A1).**

52.      Regarding claim 45, Pickup through Abkemeier taught the method for filtering spam in a

messaging system in claim 33. Pickup through Abkemeier teach confirming that message sender

can receive one or more message, distributing information with other plurality of spam filters in

the message system, using said distributing information to determined if a message should be

send to intended recipient without separately confirmation ("the sender is added to the list of

authorised senders and the electronic mail is forwarded to the recipient" see Pickup: ¶[0011]).

Pickup further teaches wherein the information is maintained in a list that includes one or more

confirmed message senders ("there are a plurality of recipients, and **each recipient has a list of authorised senders**" see Pickup: ¶[0016]) and associating a passcode with one or more of the confirmed senders in the list, and verifying a message received from a sender in the list including verifying the passcode specified by the sender (see Pickup: ¶[0022]).

Pickup through Abkemeier does not explicitly disclose prompting a sender in the list to enter a passcode upon an occurrence of an predefined event.

Brown teaches prompting a sender in the list to enter a passcode upon an occurrence of an predefined event (the process passes to block 808 which depicts the client email application prompting the sender to enter a passcode for the intended recipient see Brown: ¶[0053]).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup through Brown before them at the time the invention was made to modify the method for filtering email system of Pickup and Fleming to include prompting a sender in the list to enter a passcode upon an occurrence of an predefined event as taught by Brown.

One of ordinary skill in the art would have been motivated to make this modification in order to provide security purpose in view of Brown.

53.     Regarding claim 46, Pickup through Brown taught the method for detecting spam according to claim 45, as described above. Brown further teaches detecting that an email address associated with the sender has been compromised, and prompting the sender to enter the passcode thereafter (the process passes to block 808 which depicts the client email application prompting the sender to enter a passcode for the intended recipient see Brown: ¶[0053]; Fig.8 blocks 806-808).

54.     Regarding claim 47, Pickup through Brown taught the method for detecting spam as described above. Brown further teaches receiving a pass code from the confirmed message sender; and verifying the pass code is included in the message prior to forwarding the message from the confirmed message the sender to the intended recipient (sender's client email application inserting a passcode directive that includes the recipient's passcode as the first line in the body of the email message and transmitting the email to the intended recipient see Brown: ¶[0054], Fig.8 Blocks 810-812).

55.     Regarding claim 48, Pickup through Brown taught the method for detecting spam according to claim 47, as described above. Brown further teaches automatically adding the passcode associated with the sender at a time for transmission of a message from the sender in the messaging system (when sender compose an email message, the passcode (save in sender address book see Brown: Fig.8 block 806) will added to the email and transmit email to intended recipient see Brown: Fig.8)

56.     Regarding claim 49, Pickup through Brown taught the method for detecting spam according to claim 48, as described above. Brown further teaches providing a plug-in module for automatically adding the passcode, the plug-in module adapted to add the passcode prior to transmission to the messaging system (Features that added to adding the passcode to the normal email program that consider as plug in module see Brown: Fig.8 and Fig.10).


57.     **Claims 50-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pickup (US 2003/0212791 A1) in view of Fleming et al. (US 6,249,805) in view of Abkemeier (US 2003/0023736 A1) and further in view of Rounthwaite et al. (US 7,219,148).**

58.     Regarding claim 50, Pickup through Abkemeier taught method for filtering spam in claim

33 as described as hereinabove. Pickup further teaches correlating sender-recipient data at a

spam filter in the messaging system and determining a list of unacceptable senders using the

sender-recipient data and the determined data (Blacklist see Fig.1); and sharing the list of

unacceptable senders with other spam filters in the messaging system (sharing the whitelist and

blacklist withal the recipient "a plurality of recipients share the same list of authorised senders"

see Pickup: ¶0016]).

        Rounthwaite teaches determining data related to how fast a list of recipients grows for a

given sender (determining spammer based on the limitations "there may be limitations on the

number of messages selected per user or per user per time period, or on the probability of

selecting a message from any given user. Without such limits, a spammer could create an

account" see Rounthwaite: col.6 lines 62-66).

        It would have been obvious to one of ordinary skill in the art, having the teachings of

Pickup and Rounthwaite before them at the time the invention was made to modify the method

for filtering system of Pickup to include determining data related to how fast a list of recipients

grows for a given sender as taught by Ref B.

        One of ordinary skill in the art would have been motivated to make this modification in

order to determining whether the senders is spammer or not based on the statistics in view of

Rounthwaite.

59.     Regarding claim 51, Pickup through Rounthwaite taught the method for detecting spam

according to claim 33, as described above. Pickup further teaches maintaining a list of recipients

for each sender of messages processed by a given spam filter (each recipient has a whitelist and

blacklists "each recipient has a list of authorised senders" See Pickup: ¶[0016]; Fig.1) .

60.     Regarding claim 52, Pickup through Rounthwaite taught the method for detecting spam

according to claim 33, as described above. Pickup further teaches maintaining the list of

recipients for each sender at a data center (the whitelist at the server will be automatic update and

share with other recipients "To automatically update the whitelist, the recipient can utilise the

automatic updating mechanism of the present invention" see Pickup: ¶[0062]).


## *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action.  Accordingly, **THIS ACTION IS MADE FINAL**.  See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action.  In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action.  In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Guang Li whose telephone number is (571) 270-1897. The

examiner can normally be reached on Monday-Friday 8:30AM-5:00PM(EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Jeff Pwu can be reached on (571) 272-6798. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


April 28, 2009
GL
Patent Examiner


/Jeffrey  Pwu/

Supervisory Patent Examiner, Art Unit

2446